BITCOIN POUR REMPLACER LES DEVISES ?

FRANÇOIS R. VELDE*

Les dernières années ont vu l'émergence de ce que l'on peut appeler des monnaies digitales ou virtuelles. Cette innovation est venue du secteur privé et nul ne sait encore où elle mènera. Les banques centrales doivent-elles s'en inquiéter ? Quelles en sont les conséquences monétaires et financières ?

Dans cet article, nous décrirons Bitcoin, qui est sans doute la monnaie digitale la plus notoire. Une description précise est nécessaire pour bien comprendre la nature de cette monnaie. Il faut aussi garder présent à l'esprit l'inspiration derrière Bitcoin, qui est de résoudre un problème : comment créer une monnaie fiable, mais décentralisée ? Quoiqu'on pense de ce problème, la solution apportée a le mérite d'être innovatrice et la portée de ces innovations peut aller au-delà du problème précis.

DU PROTOCOLE DE COMMUNICATION SUR INTERNET AU MOYEN DE PAIEMENT

Bitcoin est un protocole de communication, c'est-à-dire un ensemble de règles que ses utilisateurs acceptent de suivre afin d'envoyer et de recevoir des données. Un autre exemple de protocole est http qui gouverne la façon dont les serveurs du web et les clients (c'est-à-dire les logiciels comme Internet Explorer, Chrome, Firefox, etc.) communiquent entre eux. Ce préalable comporte plusieurs éléments. D'abord, Bitcoin est une forme d'interaction sur Internet, qu'il présuppose. Ensuite, l'utilisation de Bitcoin, c'est-à-dire de ce protocole, est pure-

* Banque de Réserve fédérale de Chicago. Contact : fvelde@frbchi.org.

ment volontaire. Enfin, le bitcoin[1], en tant que monnaie, est le résultat des interactions entre les utilisateurs de ce protocole.

La façon la plus simple de présenter le protocole est de le décrire de façon récursive. Supposons qu'Auguste possède des bitcoins, gérés par un logiciel de portefeuille, et désire les céder à Béatrice. Auguste donne à son logiciel l'adresse de Béatrice. Le logiciel construit un message qui contient l'adresse d'Auguste, celle de Béatrice et le montant cédé, puis il transmet ce message au réseau. Chaque nœud du réseau qui reçoit le message en évalue la validité. En particulier, il vérifie qu'Auguste est bien le propriétaire des bitcoins en consultant la liste de toutes les transactions passées (nous verrons bientôt comment cette liste est constituée). Si le message est validé, le nœud l'ajoute à la zone mémoire avec d'autres messages récemment diffusés et le transmet à son tour. Le message est ainsi propagé à l'ensemble du réseau et fait partie de la mémoire collective du réseau qui contient les transactions en attente de confirmation.

La suite du processus, c'est-à-dire la confirmation, se déroule maintenant sur le réseau, dont certains nœuds exercent une activité dite « minière ». Celle-ci consiste à prendre un ensemble de transactions en attente à la liste, en former un bloc et à l'ajouter à la liste des transactions passées. La liste n'est pas gérée de façon centrale par une quelconque autorité. Chaque nœud détient un exemplaire de cette liste et la met à jour en ajoutant un bloc. Mais un bloc ne peut être ajouté aux blocs précédents que s'il possède une propriété particulière : il doit comporter dans son en-tête, outre le résumé des transactions qu'il contient, la solution à un problème mathématique. L'activité minière consiste à chercher la solution à ce problème et chaque nœud est libre de s'y employer.

Le problème mathématique est au cœur du protocole et mérite donc d'être décrit en plus de détails. Il repose sur ce que l'on appelle une fonction de hachage, à savoir une fonction qui prend une séquence de lettres et de chiffres x de longueur arbitraire, et en tire une autre y de longueur fixe. La propriété des fonctions de hachage est qu'il est relativement facile de calculer y à partir de x, mais impossible de retrouver x à partir de y, de même qu'il est difficile de factoriser (décomposer en un produit de nombres premiers) un grand nombre, mais facile de vérifier qu'une factorisation est correcte. Le problème mathématique est alors le suivant : étant donné l'en-tête du bloc le plus récent x, il faut trouver un nombre n (dit « valeur de circonstance ») tel que le hachage y de la séquence $\{x, n\}$ satisfasse une certaine condition : par exemple, les vingt-cinq premiers caractères doivent être des zéros. Comme il n'est pas possible d'aller à l'envers et de calculer n, la seule méthode consiste à essayer des nombres n les uns après les autres, jusqu'à ce que l'on trouve un y qui réponde à la condition.

Chaque mineur s'attelle donc à la tâche et cherche à trouver le nombre *n*. Le premier qui trouve le fait aussitôt savoir au réseau. Chaque nœud du réseau peut facilement vérifier que la solution proposée est la bonne et ajouter le bloc (avec sa solution dans l'en-tête) à la chaîne des blocs passés. Mais pourquoi les mineurs s'évertuent-ils à trouver la solution ? Parce que le gagnant a droit à une récompense. Dans son bloc gagnant, il lui est permis d'insérer une transaction très particulière (nommée *coinbase*), qui transfère un nombre fixe de bitcoins de personne à lui-même. C'est d'ailleurs la seule façon de créer des bitcoins.

Deux aspects du protocole régulent les mineurs. Premièrement, la condition que doit satisfaire le hachage change tous les 2 016 blocs. La nouvelle condition est ajustée en fonction du temps qu'il a fallu pour ajouter ces 2 016 blocs : s'ils sont ajoutés trop vite (par exemple, parce que des mineurs plus puissants sont en lice), la difficulté du problème augmente (par exemple, il faut 26 zéros au lieu de 25), de façon à maintenir le temps moyen entre deux blocs aux alentours de dix minutes. Par ailleurs, la récompense reste fixe jusqu'à ce que 210 000 blocs aient été ajoutés (ce qui prend environ quatre ans), après quoi elle diminue de moitié. Elle a commencé à 50 bitcoins, est actuellement de 25 bitcoins et doit diminuer à nouveau courant 2016. Elle continuera ainsi à diminuer de moitié jusqu'à atteindre la limite de divisibilité du bitcoin (10^{-8}). Puisque l'activité minière est la seule source de nouveaux bitcoins, il s'ensuit que la quantité totale de bitcoins croît de plus en plus lentement et, comme la flèche de Zénon, approche, mais sans jamais atteindre, le total de 21 millions.

Que se passe-t-il lorsque la récompense devient trop petite ? Il existe un autre moyen de récompenser les mineurs. L'une des règles de validité d'une transaction est que la somme des bitcoins en entrée doit être supérieure ou égale à celle des bitcoins en sortie. La différence, s'il y en a une, rémunère le mineur. Ces rémunérations prendront à terme le relais de la récompense fixe dans la motivation des mineurs.

On voit maintenant le rôle que joue la chaîne de blocs. Elle contient toutes les transactions depuis le commencement de Bitcoin ; elle est connue de et choisie par tous les nœuds du réseau, qui accepte par convention la chaîne qui incorpore la plus grande quantité d'efforts (c'est-à-dire, en pratique, la chaîne la plus longue) comme seule chaîne authentique.

Si quelqu'un voulait falsifier la chaîne de blocs, il le pourrait, à condition de diffuser une chaîne de blocs plus longue que la vraie. Par exemple, si la chaîne avait une longueur de 908 et qu'il voulait la falsifier à partir du bloc 903, il lui faudrait créer 6 blocs (les faux blocs 904 à 908 et un bloc supplémentaire). Mais créer ces blocs prendrait du temps, puisqu'il faudrait résoudre six fois le problème de hachage,

et pendant ce temps, le reste du réseau continuerait à allonger la chaîne, au rythme d'un bloc toutes les dix minutes. Le falsificateur serait engagé dans une course contre le reste du réseau. C'est ici la force du concept de *proof of work* : pour être malhonnête, il faut faire encore plus d'efforts coûteux que pour être honnête.

Le système n'est cependant pas invulnérable. En effet, pour créer un bloc valide, il faut résoudre le problème de hachage, qui ne peut se faire qu'en variant la valeur de circonstance à l'aveuglette. Créer un bloc est donc une loterie dans laquelle la probabilité de gagner est proportionnelle à la part du mineur dans la capacité totale de calcul du réseau. Un mineur qui aurait 51 % de cette capacité finirait toujours par gagner la course. Il pourrait même la gagner avec moins de 51 %. C'est la tactique du « mineur égoïste » qui lorsqu'il trouve un bloc avant les autres ne le révèle pas aux autres mineurs et commence tout de suite à travailler sur le bloc suivant. Avec 33 % de la capacité totale, il pourrait construire en secret une chaîne plus longue que celle sur laquelle travaillent les autres, et donc imposer la sienne au moment voulu, puisque le consensus se porte toujours sur la chaîne la plus longue. Dans un cas comme dans l'autre, la chaîne sur laquelle travaillait le reste du réseau deviendrait une branche morte et les transactions qui y figuraient, mais qui seraient absentes de la nouvelle chaîne créée par le falsificateur, seraient de fait annulées. Dans ce cas, le falsificateur pourrait dépenser le même bitcoin deux fois : une fois par une transaction qu'il aurait diffusée, mais exclue de sa chaîne, une deuxième fois par une transaction qu'il n'aurait pas diffusée, mais incluse dans sa chaîne.

Nous avons posé en détail les éléments du protocole. Il est maintenant possible de mieux comprendre la nature de Bitcoin.

Qu'est-ce qu'un bitcoin ? C'est, au fond, une chaîne de transactions qui commence par le *coinbase* d'un mineur chanceux et qui aboutit à son propriétaire actuel. De même qu'un billet de banque est identifié par son numéro de série, chaque bitcoin est identifié par une séquence, modifiée à chaque transaction, et la chaîne sert de cadastre[2]. L'authenticité de la chaîne est assurée par la chaîne dans laquelle chaque bloc est relié à l'en-tête du bloc précédent par sa valeur de circonstance. La chaîne est protégée de la contrefaçon par le principe du *proof of work*. Ce principe crée un coût qui est compensé par de la création monétaire. Mais il faut bien voir que la raison d'être de ce coût est la nécessité de garantir l'authenticité de la chaîne et cette nécessité découle du refus de toute autorité centrale.

Comment un bitcoin peut-il servir d'instrument monétaire ? C'est un bien qui n'existe que sous une forme numérique, dont la quantité est limitée artificiellement et dont la propriété, par construction, se transmet facilement sur Internet. Ce n'est donc pas un moyen de transférer d'autres actifs ou d'autres monnaies, dollars ou euros : c'est une valeur en

soi, mais qui n'est au passif d'aucune personne ou entité comme les valeurs bancaires et qui n'a la sanction ou la protection d'aucun gouvernement ou système légal comme les unités monétaires officielles. Aucun individu ou aucune organisation ne contrôle directement Bitcoin. Le protocole n'existe pas et les bitcoins n'ont de valeur que dans la mesure où ils sont utilisés par ceux qui choisissent d'en faire usage. Cette dernière caractéristique est en fait au cœur du concept de monnaie. Je n'accepte une monnaie en échange de biens ou de services que parce que je pense pouvoir trouver quelqu'un d'autre qui l'acceptera à son tour. Ce quelqu'un d'autre peut être l'État qui désigne quelle monnaie il accepte en paiement d'impôts ou une personne contrainte par l'État ou la loi, par exemple un créancier requis d'accepter la monnaie en paiement d'une dette. Mais on sait que la force de l'État n'est ni nécessaire, ni suffisante pour donner une valeur pérenne à une monnaie.

UN SYSTÈME DE PAIEMENT, MAIS PAS ENCORE UNE MONNAIE

Comme moyen de paiement, Bitcoin a des avantages potentiels, en grande partie dus à sa structure décentralisée. Les paiements sont relativement rapides : une transaction est confirmée en moyenne au bout de dix minutes, encore qu'il est recommandé d'attendre que plusieurs blocs aient été ajoutés à la chaîne avant d'admettre un paiement comme définitif. Le réseau, étant décentralisé, est par nature robuste. Les paiements se font de personne à personne et ne nécessitent pas d'intermédiaires, financiers ou autres – les utilisateurs gardent le choix de passer par une « banque » ou un dépositaire pour gérer leurs portefeuilles électroniques. La chaîne sur laquelle tout repose offre un témoignage inaltérable des transactions passées et peut servir de preuve. Les transactions sont irréversibles, ce qui est à la fois un avantage et un inconvénient, selon les applications. Le bitcoin étant divisible jusqu'à 10^{-8}, il rend possible les micropaiements et donc les transactions qui ne se font pas ou se font mal.

On a souvent parlé de l'utilisation de Bitcoin par les criminels. C'est indéniable, comme pour l'argent liquide d'ailleurs. Mais Bitcoin présente de sérieux inconvénients pour les criminels, puisque toutes les transactions sont enregistrées. Il est vrai que les adresses des portefeuilles seules apparaissent dans la chaîne et il faut des informations supplémentaires pour les relier à des individus. Mais si la justice dispose de ces informations (par exemple, parce qu'elle a saisi les ordinateurs des criminels), elle peut établir la preuve des transferts ; l'affaire *Silk Road* aux États-Unis l'a bien démontré.

Cela dit, Bitcoin a beaucoup d'obstacles à surmonter avant de se transformer de moyen de paiement en véritable monnaie. Son utilisation comme moyen de paiement reste marginale et la demande de

bitcoin est essentiellement spéculative, les investisseurs faisant un pari sur son succès éventuel et un fort gain en capital en conséquence. Il s'ensuit que sa valeur d'échange contre les monnaies officielles (dollar, euro) fluctue considérablement et les vendeurs qui acceptent le bitcoin ne libellent guère leurs prix en bitcoins. Peu employé comme moyen de paiement limité, risqué comme réserve de valeur, inutilisé comme unité de compte, le bitcoin est loin d'être une monnaie. Il pourrait devenir plus commun s'il devenait moins risqué, mais sa valeur ne se stabilisera que s'il devient plus couramment utilisé.

L'AVENIR DE BITCOIN ET DES AUTRES MONNAIES DIGITALES

Bitcoin reste un protocole très complexe. Il est vrai que l'on n'a pas besoin de comprendre la dynamique des fluides pour prendre un avion, mais la technologie de Bitcoin n'est pas encore mûre. Il fonctionne depuis plusieurs années, mais il a déjà connu des changements et pourra en connaître d'autres bien plus importants. Les programmes qui appliquent le protocole sont à code source ouvert, ce qui veut dire qu'ils n'appartiennent à personne et peuvent être librement examinés, voire copiés. Quand un changement est nécessaire ou souhaitable, toute personne est libre de le proposer et c'est l'ensemble des utilisateurs qui décidera s'il est accepté. Pratiquement, les modifications du protocole sont entre les mains d'un petit groupe de programmeurs, mais même entre eux, il n'est pas toujours facile de parvenir à un accord sur la marche à suivre. Des scissions sont possibles au cours desquelles une partie des utilisateurs refuse d'adopter le changement que l'autre partie a accepté, avec pour résultat une bifurcation de la chaîne et une scission monétaire.

Un débat récent dans la communauté Bitcoin illustre ce problème. Il portait sur une autre limitation de Bitcoin, à savoir sa capacité. La taille des blocs est limitée par le protocole et se traduit par une limite d'environ sept transactions par seconde, capacité clairement insuffisante pour un réseau qui se voudrait global. La proposition d'augmenter la taille a soulevé des controverses et il est devenu manifeste que la communauté Bitcoin n'a pas encore de mécanisme pour les résoudre. Il serait difficile de tolérer ce genre de blocage pour une monnaie largement utilisée.

La nature du réseau Bitcoin peut aussi changer. La vision d'origine comportait des nœuds égaux entre eux, validant les transactions et minant en même temps. Le réseau a changé, côté mineurs et côté nœuds. Le bitcoin ne valait à ses débuts que quelques centimes, mais depuis l'envolée de son prix en 2012, les gains pour les mineurs (fixes en bitcoins) se sont aussi envolés. Le protocole, on l'a vu, ajuste la difficulté face à la ruée des mineurs, mais on n'avait pas prévu la course aux

armements entre mineurs. Aujourd'hui, les mineurs conçoivent des circuits intégrés qui ne servent qu'à résoudre le problème de hachage et recherchent de par le monde entier les sources d'électricité les moins chères (le coût marginal du mineur provenant entièrement de l'énergie consommée). La concentration de l'industrie minière est forte : à ce jour, une demi-douzaine d'opérateurs minent plus des deux tiers des blocs. Aucune « attaque par 51 % » n'a eu lieu à ce jour, mais les risques de cette concentration pour le modèle Bitcoin sont importants. Du côté des nœuds, le réseau a aussi changé parce que la chaîne devenant de plus en plus longue, il est peu pratique pour chaque nœud de l'examiner en entier pour chaque transaction, d'où l'émergence de nœuds simplifiés qui se contentent de demander à d'autres nœuds choisis au hasard de faire une partie du travail de vérification. La proportion de nœuds complets se réduit donc, ce qui pose un risque de fragilité.

Enfin, Bitcoin est loin d'être la seule tentative de monnaie digitale, encore qu'il reste la principale. La concurrence est libre et nombre d'expérimentateurs ont devisé des variantes, s'inspirant généralement de Bitcoin, mais en le modifiant. Est-ce que Bitcoin ou l'une de ces « altcoins » remplacera les monnaies officielles ? Les enthousiastes des premières heures ont pu le croire, mais l'histoire montre que les États ont depuis longtemps inclus la monnaie parmi les prérogatives régaliennes et n'en ont cédé le contrôle que quand ils ne pouvaient ou voulaient l'exercer. On connaît des épisodes, comme ceux des monnaies de nécessité, où l'État a toléré que le secteur privé supplée telle portion du système monétaire et tout au plus, on peut supposer qu'une ou plusieurs monnaies digitales soient tolérées dans des emplois spécialisés. Mais si la monnaie sur papier doit connaître le même sort que le livre sur papier, c'est-à-dire être supplantée par un support plus moderne, il y a fort à parier que les États voudront se mettre à la pointe du progrès.

Mais la question n'est pas tout ou rien et au-delà des spécificités de Bitcoin, il convient de s'interroger sur la portée de cette avancée technologique.

Bitcoin, au minimum, est une expérience grandeur nature qui a démontré comment assurer l'authenticité d'un cadastre public de transactions sans contrôle central. Vu sous un angle monétaire, il permet de transférer des unités dont le nombre total est fixe, mais le mécanisme pourrait être utilisé pour transférer autre chose. C'est déjà le cas : la transaction, dans son exécution technique, comporte un programme dont le but est de vérifier au moyen d'une clé cryptographique que c'est bien le propriétaire qui initie la transaction, mais qui pourrait aussi accomplir d'autres tâches. Le langage de programmation est assez limité, mais il permet d'imposer des conditions supplémentaires, par exemple en exigeant plusieurs signatures ou en distribuant les bitcoins transférés vers

différents destinataires si certaines conditions sont remplies. Cela nous mène au concept de « contrats intelligents » : la chaîne de blocs pourrait devenir le support de transactions plus complexes, portant sur des objets autres que le transfert de bitcoins. C'est un peu comme si l'on utilisait des billets de banque comme supports pour écrire et exécuter des contrats sur d'autres avoirs. Le projet Ethereum est une tentative de reconstruire le bitcoin dans ce sens, en permettant d'obtenir des données extérieures au système (par exemple, la température dans un endroit donné ou le prix d'un actif) et de conditionner les transferts à ces données.

Il existe d'autres systèmes de paiement qui reposent sur une structure décentralisée, mais qui laissent de côté le *proof of work*. Tel est le cas de Ripple où la validation des transactions se fonde sur l'obtention d'un consensus. Chaque nœud du réseau gère une liste de nœuds auxquels il fait confiance et l'état de la chaîne est modifié lorsqu'on atteint un consensus (80 % des nœuds) à la suite d'un processus itératif. Ripple retient le concept de monnaie « indigène » au système, et ce, à des fins de sécurité : chaque transaction consomme des unités de valeurs, assez faibles pour ne pas imposer de coût aux transactions légitimes, mais assez pour décourager un flot de fausses transactions.

On sait que les banques privées s'intéressent de plus en plus à la chaîne de blocs. Il est encore trop tôt pour savoir où s'orientent ces recherches, mais il semble que l'idée d'une gestion décentralisée des balances, permettant des transactions de pair à pair, au moyen d'une chaîne à l'authenticité incontestable, comporte de grands attraits. Le protocole Bitcoin résout un problème qui n'est pas celui des banques, à savoir établir une monnaie fiable sans autorité centrale. Mais le succès (relatif) du protocole a mis en avant un ensemble de techniques cryptographiques et informatiques qui, si elles ne sont pas neuves, n'avaient pas été considérées dans leur totalité. L'enjeu pour les banques centrales ne tient plus à leur fonction de créateurs de monnaie, mais plus à leur rôle dans les systèmes de paiement, aussi bien comme régulateurs que comme garantes de la stabilité financière et comme détenteurs du moyen de paiement ultime, la monnaie légale. Si une monnaie doit jouer un rôle clé dans ces systèmes décentralisés, il serait naturel que les banques centrales veillent à ce que cette monnaie soit la leur.

NOTES

1. Par convention, Bitcoin désigne le protocole et le bitcoin l'unité monétaire.

2. On parle souvent de registre ou de grand livre, mais la chaîne n'est pas organisée en comptes (même si elle contient toute l'information nécessaire pour reconstituer les comptes de tous les possesseurs).